0418017-SNY

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－202766

(43)公開日　平成11年(1999)７月30日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６７５Ｂ

審査請求　未請求　請求項の数15　ＯＬ　（全 15 頁）

(21)出願番号　特願平10－6629

(22)出願日　平成10年(1998)１月16日

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号

(72)発明者　大石　和臣
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

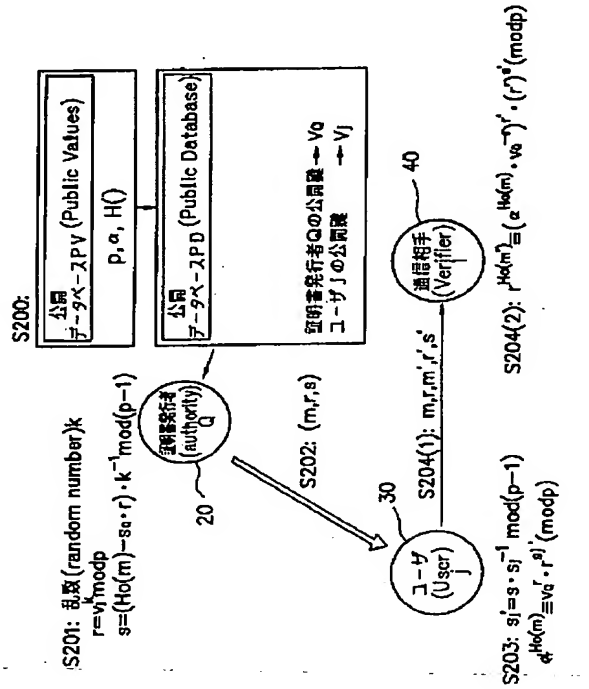
(74)代理人　弁理士　國分　孝悦

(54)【発明の名称】　ディジタル署名方式、それを用いた情報通信システム及び通信装置

(57)【要約】

【課題】　如何なる場合でも匿名性を確実に保つことができるディジタル署名方式を用いた情報通信システムを提供する。

【解決手段】　手段２０は、共通に使用する公開パラメータＰＶの代わりに、ユーザの公開情報ｖｊを用い、ディジタル情報ｍに対するディジタル署名ｒ，ｓを生成する。手段３０は、ディジタル署名ｒ，ｓを秘密情報ｓｊを用いて変換することで別の値を求め、ディジタル情報ｍ、ディジタル署名ｒ，ｓ、公開パラメータＰＶ、及び公開鍵ｖQ から得られる値を公開情報と見なし、且つ、ディジタル署名ｒ，ｓを変換して得られた別の値をそのユーザの秘密情報と見なすことで、離散対数問題に安全性の根拠を置く公開鍵暗号を利用する。



【特許請求の範囲】
【請求項１】　各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、
ディジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記ディジタル情報に対応する署名を生成する署名生成ステップと、
上記公開パラメータ及び上記公開情報を用いて、上記ディジタル情報と上記署名の対応関係が正しいか否かを判別する署名判別ステップとを含むディジタル署名方式であって、
上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、
上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、
上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、ディジタル情報を暗号化する暗号化ステップとを含むことを特徴とするディジタル署名方式。
【請求項２】　上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、上記暗号化ステップで暗号化して得られた暗号文を復号する復号ステップを含むことを特徴とする請求項１記載のディジタル署名方式。
【請求項３】　各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、
ディジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記ディジタル情報に対応する署名を生成する第１の署名生成ステップと、
上記公開パラメータ及び上記公開情報を用いて、上記ディジタル情報と上記署名の対応関係が正しいか否かを判別する第１の署名判別ステップとを含むディジタル署名方式であって、
上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、
上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、
上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、ディジタル情報に対応する署名を生成する第２の署名生成ステップとを含むことを特徴とするディジタル署名方式。
【請求項４】　上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、上記第２の署名生成ステップで生成された署名とそれに対応したディジタル情報の関係が正しいか否かを判別する第２の署名判別ステップを含むことを特徴とする請求項３記載のディジタル署名方式。
【請求項５】　複数のユーザ間で共通に用いられる底の値に対して、各ユーザの秘密情報を指数値として指数計算した結果を、各ユーザの公開情報とする公開情報ステップを含むディジタル署名方式であって、
ユーザの公開情報を共通の底の代わりに用いて生成した平文に対する署名、及び上記ユーザの秘密情報を基に、そのユーザの新たな秘密情報を生成する秘密情報生成ステップと、
上記秘密情報生成ステップで生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成ステップと、
上記署名、上記ユーザの公開情報、上記共通の底、及び上記平文から、上記ユーザの新たな公開情報を生成する公開情報生成ステップと、
上記秘密情報生成ステップで生成された新たな秘密情報、上記パラメータ生成ステップで生成された新たなパラメータ、及び上記公開情報生成ステップで生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行ステップとを更に含むことを特徴とするディジタル署名方式。
【請求項６】　離散対数を求めることの困難性に安全性の根拠を置くディジタル署名方式を含むことを特徴とする請求項５記載のディジタル署名方式。
【請求項７】　上記ディジタル署名方式は、ＥｌＧａｍａｌ署名方式を含むことを特徴とする請求項６記載のディジタル署名方式。
【請求項８】　上記ディジタル署名方式は、ＥｌＧａｍａｌ署名方式の変形を含むことを特徴とする請求項６記載のディジタル署名方式。
【請求項９】　上記公開鍵暗号は、離散対数を求めることの困難性に安全性の根拠を置く暗号を含むことを特徴とする請求項５記載のディジタル署名方式。
【請求項１０】　請求項１～９の何れかに記載のディジタル署名方式を用いた情報通信システムであって、
第１のユーザが第２のユーザに対して、毎回異なる新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成可能なユーザ情報生成手段と、
上記第２のユーザに対する情報が、上記第１のユーザが上記ユーザ情報生成手段により生成したものであることを確認するユーザ情報確認手段と、
上記ユーザ情報確認手段で確認された情報を用いて、公開鍵暗号を実行する公開鍵暗号実行手段とを含み、
上記ユーザ情報生成手段により生成された新たなパラメータ、及び新たな公開情報から、それらに対応するユーザが情報量的に判定不可能であることを特徴とする情報通信システム。
【請求項１１】　ユーザに共通の公開パラメータ及びユーザに固有の秘密情報からユーザに固有の公開情報を生

成する公開情報生成手段と、
上記公開パラメータ及び上記公開情報を用いて、送信されてきたディジタル情報と、そのディジタル情報に対応する署名との対応関係が正しいか否かを判別する署名判別手段と、
上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成手段と、
上記ユーザ情報生成手段で生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認手段と、
上記確認手段で確認された新たなパラメータ及び新たな公開情報を用いて、ディジタル情報を暗号化する暗号化手段とを備えることを特徴とするディジタル署名方式の通信装置。
【請求項１２】　上記確認手段で確認された新たなパラメータ及び新たな秘密情報を用いて、ディジタル情報に対応する署名を生成する署名生成手段を備えることを特徴とする請求項１１記載の通信装置。
【請求項１３】　複数のユーザ間で共通に用いられる底の値に対して、ユーザの秘密情報を指数値として指数計算した結果を、ユーザの公開情報とする公開情報手段と、
上記公開情報を共通の底の代わりに用いて生成したディジタル情報に対する署名、及び上記秘密情報を基に、新たな秘密情報を生成する秘密情報生成手段と、
上記秘密情報生成手段で生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成手段と、
上記署名、上記公開情報、上記共通の底、及び上記ディジタル情報から、新たな公開情報を生成する公開情報生成手段と、
上記秘密情報生成手段で生成された新たな秘密情報、上記パラメータ生成手段で生成された新たなパラメータ、及び上記公開情報生成手段で生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行手段とを備えることを特徴とするディジタル署名方式の通信装置。
【請求項１４】　上記ディジタル署名方式は、請求項１～９の何れかに記載のディジタル署名方式であることを特徴とする請求項１１～１３の何れかに記載の通信装置。
【請求項１５】　請求項１１～１４の何れかに記載の通信装置を含むことを特徴とする情報通信システム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、公開鍵暗号を用いたディジタル署名方式、それを用いた情報通信システム及び通信装置に関するものである。
【０００２】
【従来の技術】例えば、コンピュータと通信ネットワークの発展と広範な普及に伴い、従来は通信ネットワーク上で実現できなかった社会的活動等、多様な機能が実現できるようになった。しかしながらその反面、誰が、いつ、どこで、何を行ったのかを容易に把握される場合があった。そこで、これを防ぐために、匿名で通信処理を行うことで、プライバシーを保護し、且つ通信ネットワーク上で多様な機能を実現する方法が提案されている。
【０００３】このような方法としては、例えば、公開鍵暗号を用いた方法があり、これにより、送信者は、通信内容を意図する受信者のみに送信でき、しかも受信者は、受信した通信内容の送信者が誰であるかを確実に確認することが可能となる。そして、この方法を適用したものとしては、特願平８－１０８２２５号に開示されているディジタル署名方式及びそれを用いた情報通信システムがある。
【０００４】ここで、「暗号」及び「匿名公開鍵証明書」について具体的に説明する。
【０００５】（１）「暗号」
まず、「暗号」とは、情報の意味が当事者以外にには認識できないように情報を変換することをいう。そして、この暗号においては、元の文（変換されていない文）を「平文」といい、その平文を第三者に意味の分からない文（暗号文）に変換することを「暗号化」といい、その変換の手順を「暗号アルゴリズム」という。平文及び暗号文は、テキストデータに限られるものではなく、音声や画像等、あらゆる情報を想定している。暗号化は、「暗号化鍵」と呼ばれるパラメータに依存する変換である。そして、その暗号化で得られた暗号文を当事者が元の平文に戻すことを「復号」といい、その復号の際には、「復号鍵」と呼ばれる暗号化鍵に対応するパラメータが用いられる。一方、当事者以外の第三者が暗号文を元の平文に戻すこと、或いは、復号鍵を見いだすことを「解読」という。
【０００６】上述のような暗号では暗号の安全性を、暗号化に用いる暗号化鍵或いは復号に用いる復号鍵に帰着させており、それらの鍵を知らなければ、たとえ暗号アルゴリズムを知っていても、平文は得られないようになっている。したがって、所定の暗号化を行う装置（暗号装置）の製造者でも、解読不可能な暗号化を実現することができる。
【０００７】また、暗号には、多くの暗号アルゴリズムがある。そこで、例えば、暗号化鍵を公開できるか否かの観点から、暗号を、非対称暗号（公開鍵暗号）と対称暗号（共通鍵暗号）の２つに分類して説明する。
【０００８】（１－１）「非対称暗号（公開鍵暗号）」
「非対称暗号」とは、「公開鍵暗号」とも呼ばれ、暗号化鍵と復号鍵が異なり、暗号化鍵から復号鍵が容易に計算して得られないようになっており、また、暗号化鍵を公開し、復号鍵を秘密に保持して使用される暗号のことをいう。このような非対称暗号は、以下のような特徴を

持っている。
特徴１：暗号化鍵と復号鍵が異なり、暗号化鍵が公開されるため、暗号化鍵を秘密に配送する必要がなく、その鍵の配送が容易である。
特徴２：各利用者の暗号化鍵は公開されるため、各利用者は、各自の復号鍵のみ秘密に保持しておけばよい。
特徴３：送信されてきた通信文の送信者が偽者でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証（ディジタル署名）機能を実現できる。
【０００９】ここで、暗号機能と上述の認証機能を実現できる非対称暗号としては、ＲＳＡ暗号（R.L.Rivest, A.Shamir and L.Adleman,"A method of obtaining digital signatures and public key cryptosystems,"Communications of ACM, Vol.21, No.2, pp.120-126, 1978 ）や、ＥＩＧａｍａｌ暗号（T.E.ElGamal,"A public key cryptosystem and a signature scheme based on discrete logarithms,"IEEE Transaction on Information Theory, Vol.IT-31, No.4, pp.496-472, 1985 ）が知られている。また、認証機能を実現できる非対称暗号としては、Ｆｉａｔ－Ｓｈａｍｉｒ暗号（A.Fiat, A.Shamir,"How to prove yourself:practical solutions of identification and signature problrms,"Proc. of CRYPTO'86, 1987 ）や、Ｓｃｈｎｏｒｒ暗号（C.P.Schnorr,"Efficient signature generation by smart cards,"Journal of Cryptology, vol.4, pp.161-174, 1991 ）が知られている。
【００１０】例えば、ＥＩＧａｍａｌ暗号における暗号化、復号、認証（ディジタル署名）の生成、及びその検証について具体的に説明する。
【００１１】まず、「Ｚ」を整数全体の集合、「Z_p」を０以上ｐ未満の整数の集合、「$Z_p \setminus \{0\}$」をZ_pから０を除いた集合、「Z_p^*」をZ_pの要素且つｐと互いに素である整数の集合として表すものとする。また、整数Ａ，Ｂ，Ｃに対して、
Ａ＝ＢｍｏｄＣ
なる関係が成り立つとき、ＢをＣで割ったときの余りがＡであること（任意の整数ｋが存在し、「Ｂ＝ｋ・Ｃ＋Ａ」が成り立つこと）を意味し、
Ａ≡Ｂ（ｍｏｄＣ）
なる関係が成り立つとき、ＡをＣで割ったときの余りと、ＢをＣで割ったときの余りとが等しいことを意味するものとする。さらに、通信相手と共通の公開パラメータとしては、素数ｐ、Z_p^*の要素であり且つ位数ｐ－１のα、及び一方向性ハッシュ関数$H_0 : Z \rightarrow Z_p \setminus \{0\}$を用いる。また、任意のユーザｉの復号鍵（秘密鍵）を「$s_i \in Z_{p-1}$」とし、暗号化鍵（公開鍵）を「$v_i = \alpha^{s_i} \bmod p$」とする。尚、「一方向性ハッシュ関数」とは、衝突を起こしにくい圧縮関数のことである。すなわち、「一方向性ハッシュ関数」とは、任意の長さのビット列を出力する関数であり、同じ出力となる入力を見つけることが困難である、という特徴を持っている。
【００１２】①暗号化
そこで、ユーザｊが平文（メッセージ）ｍ（$\in Z_p$）を暗号化してユーザｉに対して送信する場合、ユーザｊ用端末装置では、以下のステップ１～ステップ４の手順でその処理が行われる。尚、メッセージｍがZ_pの要素でない場合、すなわちｐ以上の数値の場合には、そのメッセージｍをZ_pの要素となるようにブロック分割され、各ブロックに対して、以下の手順の暗号化が行われる。
ステップ１：ユーザｊ用端末装置は、乱数ｋを生成する。
ステップ２：ユーザｊ用端末装置は、
$C_1 = \alpha^k \bmod p$
なる計算を行う。
ステップ３：ユーザｊ用端末装置は、
$C_2 = m \cdot v_j^k \bmod p$
なる計算を行う。
ステップ４：ユーザｊ用端末装置は、ステップ２及び３の計算結果C_1及びC_2を、ユーザｉ用端末装置に対して送信する。
【００１３】②復号
上記①暗号化により、ユーザｊ用端末装置からユーザｉ用端末装置には、C_1及びC_2が送信される。そして、ユーザｉ用端末装置は、ユーザｊ用端末装置から送信されてきたC_1及びC_2を用いて、メッセージｍを、
$m = C_2 / C_1^{s_i} \bmod p$
なる計算により求める。
【００１４】③ディジタル署名の生成
上記②復号により得られたメッセージｍ（$\in Z$）に対して、ユーザｉ用端末装置がディジタル署名を生成する場合、ユーザｉ用端末装置では、以下のステップ１～ステップ４の手順でその処理が行われる。尚、上記①暗号化で述べたように、メッセージｍをブロック分割する場合もあるが、ここでは、一方向性ハッシュ関数を用いる場合を説明する。
ステップ１：ユーザｉ用端末装置は、乱数ｋ（$\in Z_{p-1}^*$）を生成する。
ステップ２：ユーザｉ用端末装置は、
$r = \alpha^k \bmod p$
なる計算を行う。
ステップ３：ユーザｉ用端末装置は、
$s = (H_0(m) - s_i \cdot r) \cdot k^{-1} \bmod (p-1)$
なる計算を行う。
ステップ４：ユーザｉ用端末装置は、ステップ２及び３の計算結果ｒ及びｓを、検証者に対して送信する。
【００１５】④ディジタル署名の検証
そして、上記③ディジタル署名の生成により得られたディジタル署名を、ユーザｉ用端末装置が検証する場合、ユーザｉ用端末装置は、

$\alpha^{H0(m)} \equiv v_j^{r} \cdot r^{S} \pmod{p}$
なる関係が成り立つか否かを確認する。

【００１６】（１－２）「対称暗号（共通鍵暗号）」
一方、「対称暗号」とは、「共通鍵暗号」とも呼ばれ、暗号化鍵と復号鍵が同一である暗号のことをいう。また、１９７０年後半に上述した非対称暗号（公開鍵暗号）が現れてから、従来から存在するこの対称暗号は、「慣用暗号」とも呼ばれるようになった。このような対称暗号は、適当な長さの文字列（ブロック）毎に同じ暗号化鍵で暗号化するブロック暗号と、文字列又はビット毎に暗号化鍵を変えて暗号化するストリーム暗号とに分類される。ブロック暗号としては、文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に換える換字式暗号等があり、ＤＥＳ（Data Encryption Standard）や、ＦＥＡＬ（Fast data Encipherment Algorithm）といった商用暗号として広く用いられている。ストリーム暗号は、メッセージに乱数をＸＯＲ（排他論理和）して、その内容を撹乱する暗号であり、このストリーム暗号としては、無限周期の乱数列を１回限りの使い捨て鍵として用いるバーナム暗号が知られている。

【００１７】尚、上述した（１）暗号の更なる詳細は、「暗号理論入門」（岡本栄司著：共立出版）や、「Applied cryptography second edition:protocols,algorithms,and source code in C」（Schneier著）、「John Wiley&;Sons,Inc」等に述べられている。

【００１８】（２）「匿名公開鍵証明書」
つぎに、「匿名公開鍵証明書」とは、上述した（１－１）非対称暗号（公開鍵暗号）等において、任意のユーザと、そのユーザの公開鍵（暗号化鍵）との対応を保証するものである。具体的には、「Certification Authority」と呼ばれる信頼できる特別なユーザ（以下、ＣＡと言う）が、他のユーザ（以下、ユーザｊとする）の身元を、例えば、パスポートで確認し、ユーザｊの識別情報ＩＤ（氏名、性別、生年月日等の個人識別情報）、その公開鍵及び有効期限等を内容とするメッセージに対するディジタル署名を生成する。このディジタル署名が「匿名公開鍵証明書」である。ＣＡの公開鍵は、誰でも確実に入手できるようになされており、ＣＡにて生成されたディジタル署名を検証することは容易である。これにより、例えば、ユーザｋがユーザｊと通信する際に、ユーザｊに対応する公開鍵を容易に且つ確実に確認することができると共に、他のユーザがユーザｊになりすますことを防ぎながら、公開鍵暗号による通信を可能とすることができる。

【００１９】また、「匿名公開鍵証明書」とは、上述の匿名公開鍵証明書のユーザが、どこの誰であるかを分からないようにしたものでもある。これにより、プライバシー保護を要する用途、例えば、ある特別なサービスを受けることができる資格を有するが、身元を明かすことを防ぎたい場合に用いることができる。これを適用したものとしては、例えば、特願平８－１０８２２６号に開示されているグループ署名と呼ばれる特殊なディジタル署名方式がある。

【００２０】上述のような匿名公開鍵証明書を適用したものとしては、例えば、特願平８－１０８２２５号に開示されている通信システムがある。この通信システムでは、図５に示すようなステップＳ５００～Ｓ５０４の処理が行われる。以下、ステップＳ５００～Ｓ５０４について具体的に説明する。尚、以下の説明における各記号（「Ｚ」や「Z_p」等）は、上述したＥＩＧａｍａＩ暗号の説明での各記号と同様に定義して用いるものとする。

【００２１】ステップＳ５００：先ず、システム共通の公開パラメータＰＶ（Public Vaiues）としては、素数ｐ、位数ｑ（但し、ｑ｜ｐ－１）、Z_p^*の要素であり且つ位数ｑのα、一方向性ハッシュ関数H_1：$Z_q \times Z \rightarrow \{0, \cdots, 2^t - 1\}$を用いる。すなわち、ｑは、ｐ－１を割り切り、$x \in Z_q \setminus \{0\}$に対して$\alpha^x \equiv 1 \pmod{p}$ではなく、且つ$x = q$に対して$\alpha^x \equiv 1 \pmod{p}$であり、$H_1$は、$Z_q$の要素とＺの要素を入力とし$2^t - 1$以下の非負整数を出力する。そして、これらのパラメータは、この通信システムに参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースＰＤ（Public Database）に登録されているものとする。そこで、証明書発行者（authority）Ｑ用端末装置７０は、復号鍵（秘密鍵）s_Qと、暗号化鍵（公開鍵）v_Q（$v_Q = \alpha^{-s_Q} \bmod p$）とを生成し、公開鍵$v_Q$を公開データベースＰＤに登録する。また、ユーザ（User）ｊ用端末装置８０は、復号鍵（秘密鍵）s_jと、暗号化鍵（公開鍵）v_j（$v_j = \alpha^{-s_j} \bmod p$）とを生成し、公開鍵$v_j$を公開データベースＰＤに登録する。

【００２２】ステップＳ５０１：匿名公開鍵証明書の生成
次に、証明書発行者Ｑ用端末装置７０は、ユーザｊの公開鍵v_jを、乱数（random number）ｒを用いて変換したｚを求め、このｚに対する署名（Ｓｃｈｎｏｒｒ暗号によるディジタル署名）を生成する。具体的には、証明書発行者Ｑ用端末装置７０は、乱数（秘密の乱数）ｒ（$r \in Z_q \setminus \{0\}$）を選択し、
$x = \alpha^r \bmod p$
$z = v_j^r \bmod p$
$e = H_1(x, z_j)$
$y = r + e \cdot s_Q \bmod q$
なる計算を行う。このＳｃｈｎｏｒｒ暗号によるディジタル署名（ｙ，ｅ，ｚ）が匿名公開鍵証明書である。

【００２３】ステップＳ５０２：匿名公開鍵証明書の配送
次に、証明書発行者Ｑ用端末装置７０は、上述のステッ

プＳ５０１にて生成した匿名公開鍵証明書（ｙ，ｅ，ｚ）を、ユーザｊ用端末装置８０に対して送信する。これを受けたユーザｊ用端末装置８０は、ｅ及びｚを、

$e = H_1(\alpha^y \cdot v_Q^e \bmod p, z)$

$z = (\alpha^y \cdot v_Q^e \bmod p)^{-S_j} \bmod p$

が成り立つことを確認する。尚、ここでは、$x = \alpha^y \cdot v_Q^e \bmod p$が成り立つことにより、表記の簡略化のためにｘを用いるものとする。

【００２４】ステップＳ５０３：公開鍵暗号の利用

次に、ユーザｊ用端末装置８０は、αとｖｊの代わりにｘとｚを用いて、離散対数問題に基づく公開鍵暗号を利用する。例えば、Ｓｃｈｎｏｒｒ暗号によるディジタル署名を利用する場合、メッセージｍに対して、以下のようにしてディジタル署名を生成する。すなわち、ユーザｊ用端末装置８０は、秘密の乱数ｒｊ（$r_j \in Z_q^*$）を選択し、

$x_j = x^{r_j} \bmod p$

$e_j = h(x_j, m)$

$y_j = r_j + e_j \cdot s_j \bmod q$

なる計算を行う。そして、ユーザｊ用端末装置８０は、メッセージｍと共に、（（ｙ，ｅ，ｚ），ｙｊ，ｅｊ，ｍ）をディジタル署名として、必要な相手に対して送信する。

【００２５】ステップＳ５０４：署名確認

そして、上述のステップＳ５０３にて送信されたディジタル署名（（ｙ，ｅ，ｚ），ｙｊ，ｅｊ，ｍ）の受信者（通信相手（Verifier））ｉ用端末装置９０は、先ず、上述のステップＳ５０２における

$e = H_1(\alpha^y \cdot v_Q^e \bmod p, z)$

なる式を確認し、次に、

$e_j = H_1(x^{y_j} \cdot z^{e_j} \bmod p, m)$

なる式を確認する。これらの確認ができた場合に、受信者ｉ用端末装置９０は、メッセージｍに対するディジタル署名は証明書発行者Ｑにより選ばれたユーザによって生成されたディジタル署名である、と認識する。

【００２６】

【発明が解決しようとする課題】ところで、上記図５の通信システムで説明したような従来の匿名公開鍵証明書では、匿名性が満たされている。すなわち、任意の匿名公開鍵証明書がどのユーザに対応するものであるのかが分からないようになっている。このような匿名性は、以下の２つの仮定に基づくものである。

【００２７】仮定１：離散対数問題

「Ｇ」を有限群とし、「α」をその生成元とする。また、「ｖ」をＧの元とし、底Ａに対するｖの離散対数を「ｌｏｇ［α］ｖ」とする。そこで、Ｇの位数（元の個数）が充分大きい場合、離散対数ｌｏｇ［α］ｖを求めることは困難となる。

【００２８】仮定２：離散対数の比較問題

「ｒ」と「ｓ」をＧのランダムな元とする。そこで、α、$v = \alpha^s$、$x = \alpha^r$、$z = \alpha^{rs}$が与えられたとき、Ｇの位数が充分大きく、ｒとｓが未知である場合、ｌｏｇ［α］ｖとｌｏｇ［ｘ］ｚが等しいか否かを判別することはできない。

【００２９】上述のような仮定１及び仮定２が成り立つことにより、匿名公開鍵証明書は匿名性が満たされる。

【００３０】しかしながら、従来では、仮定２のみを解くアルゴリズムが見いだされ、仮定１は成り立つが仮定２が成り立たず、匿名公開鍵証明書の匿名性が無くなる場合があった。

【００３１】具体的にはまず、仮定１の離散対数問題を解くことは、現在までの研究成果によれば非常に難しいとされ、安全性の根拠として用いることは妥当であると考えられている。すなわち、このような離散対数問題が解ければ、仮定２の離散対数の比較問題も解けることになる。これにより、仮定２を解くことは、仮定１を解くことと同じくらい易しい、或いは、仮定１を解くことよりも易しい、ということがわかる。したがって、この仮定２を解くことが仮定１を解くことよりどの程度易しいかは、現在のところ不明であるが、仮定２のみを解くアルゴリズムが見いだされた場合、仮定１は成り立つが仮定２が成り立たなくなるという事態が考えられる。このような場合に、上述した匿名公開鍵証明書の匿名性が無くなる。

【００３２】そこで、本発明は、上記の欠点を除去するために成されたもので、如何なる場合でも匿名性を確実に保つことができるディジタル署名方式、それを用いた情報通信システム及び通信装置を提供することを目的とする。

【００３３】

【課題を解決するための手段】本発明は、ＥｌＧａｍａｌ暗号等のディジタル署名を生成する手段と、その手段で生成されるディジタル署名を各ユーザの秘密情報を用いて変換する手段と、離散対数問題に安全性の根拠を置く公開鍵暗号を利用する手段とを少なくとも備えている。この構成において、上記ディジタル署名を生成する手段は、共通に使用する公開パラメータの代わりに、各ユーザの公開情報を用い、任意の平文や予め定められた固定値等のディジタル情報に対するディジタル署名を生成する。上記ディジタル署名を変換する手段は、上記ディジタル署名を各ユーザの秘密情報を用いて変換することで、別の値を求める。上記公開鍵暗号を利用する手段は、上記ディジタル情報、上記ディジタル署名、上記公開パラメータ、及び署名者の公開鍵から得られる値を公開情報と見なし、且つ、上記ディジタル署名を変換して得られた別の値をそのユーザの秘密情報と見なすことで、離散対数問題に安全性の根拠を置く公開鍵暗号を利用する。この公開鍵暗号を利用する手段を用いて、各ユーザは公開鍵暗号を利用する。これにより、各ユーザが公開鍵として用いる情報（公開情報）から、その情報が

どのユーザと対応するかを特定することが、情報量的に不可能となるため、匿名性は、上述の仮定２（離散対数の比較問題）に依存していない。すなわち、上記仮定２が成り立たなくなる事態が起きたとしても、匿名性は保たれる。

【００３４】すなわち、第１の発明は、各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、ディジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記ディジタル情報に対応する署名を生成する署名生成ステップと、上記公開パラメータ及び上記公開情報を用いて、上記ディジタル情報と上記署名の対応関係が正しいか否かを判別する署名判別ステップとを含むディジタル署名方式であって、上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、ディジタル情報を暗号化する暗号化ステップとを含むことを特徴とする。

【００３５】第２の発明は、上記第１の発明において、上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、上記暗号化ステップで暗号化して得られた暗号文を復号する復号ステップを含むことを特徴とする。

【００３６】第３の発明は、各ユーザに共通の公開パラメータ及び各ユーザに固有の秘密情報から、各ユーザに固有の公開情報を生成する公開情報生成ステップと、ディジタル情報に対して上記秘密情報及び上記公開パラメータを用いた変換を施すことで、上記ディジタル情報に対応する署名を生成する第１の署名生成ステップと、上記公開パラメータ及び上記公開情報を用いて、上記ディジタル情報と上記署名の対応関係が正しいか否かを判別する第１の署名判別ステップとを含むディジタル署名方式であって、上記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成ステップと、上記ユーザ情報生成ステップで生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認ステップと、上記確認ステップで確認された新たなパラメータ及び新たな秘密情報を用いて、ディジタル情報に対応する署名を生成する第２の署名生成ステップとを含むことを特徴とする。

【００３７】第４の発明は、上記第３の発明において、上記確認ステップで確認された新たなパラメータ及び新たな公開情報を用いて、上記第２の署名生成ステップで生成された署名とそれに対応したディジタル情報の関係が正しいか否かを判別する第２の署名判別ステップを含むことを特徴とする。

【００３８】第５の発明は、複数のユーザ間で共通に用いられる底の値に対して、各ユーザの秘密情報を指数値として指数計算した結果を、各ユーザの公開情報とする公開情報ステップを含むディジタル署名方式であって、ユーザの公開情報を共通の底の代わりに用いて生成した平文に対する署名、及び上記ユーザの秘密情報を基に、そのユーザの新たな秘密情報を生成する秘密情報生成ステップと、上記秘密情報生成ステップで生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成ステップと、上記署名、上記ユーザの公開情報、上記共通の底、及び上記平文から、上記ユーザの新たな公開情報を生成する公開情報生成ステップと、上記秘密情報生成ステップで生成された新たな秘密情報、上記パラメータ生成ステップで生成された新たなパラメータ、及び上記公開情報生成ステップで生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行ステップとを更に含むことを特徴とする。

【００３９】第６の発明は、上記第５の発明において、離散対数を求めることの困難性に安全性の根拠を置くディジタル署名方式を含むことを特徴とする。

【００４０】第７の発明は、上記第６の発明において、上記ディジタル署名方式は、ＥＩＧａｍａＩ署名方式を含むことを特徴とする。

【００４１】第８の発明は、上記第６の発明において、上記ディジタル署名方式は、ＥＩＧａｍａＩ署名方式の変形を含むことを特徴とする。

【００４２】第９の発明は、上記第５の発明において、上記公開鍵暗号は、離散対数を求めることの困難性に安全性の根拠を置く暗号を含むことを特徴とする。

【００４３】第１０の発明は、請求項１～９の何れかに記載のディジタル署名方式を用いた情報通信システムであって、第１のユーザが第２のユーザに対して、毎回異なる新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成可能なユーザ情報生成手段と、上記第２のユーザに対する情報が、上記第１のユーザが上記ユーザ情報生成手段により生成したものであることを確認するユーザ情報確認手段と、上記ユーザ情報確認手段で確認された情報を用いて、公開鍵暗号を実行する公開鍵暗号実行手段とを含み、上記ユーザ情報生成手段により生成された新たなパラメータ、及び新たな公開情報から、それらに対応するユーザが情報量的に判定不可能であることを特徴とする。

【００４４】第１１の発明は、ユーザに共通の公開パラメータ及びユーザに固有の秘密情報からユーザに固有の公開情報を生成する公開情報生成手段と、上記公開パラメータ及び上記公開情報を用いて、送信されてきたディジタル情報と、そのディジタル情報に対応する署名との対応関係が正しいか否かを判別する署名判別手段と、上

記公開情報を用いて、ユーザに固有の新たな秘密情報、新たなパラメータ、及び新たな公開情報を生成するユーザ情報生成手段と、上記ユーザ情報生成手段で生成された新たな秘密情報、新たなパラメータ、及び新たな公開情報が予め定められた関係を満たすことを確認する確認手段と、上記確認手段で確認された新たなパラメータ及び新たな公開情報を用いて、ディジタル情報を暗号化する暗号化手段とを備えることを特徴とする。

【００４５】第１２の発明は、上記第１１の発明において、上記確認手段で確認された新たなパラメータ及び新たな秘密情報を用いて、ディジタル情報に対応する署名を生成する署名生成手段を備えることを特徴とする。

【００４６】第１３の発明は、複数のユーザ間で共通に用いられる底の値に対して、ユーザの秘密情報を指数値として指数計算した結果を、ユーザの公開情報とする公開情報手段と、上記公開情報を共通の底の代わりに用いて生成したディジタル情報に対する署名、及び上記秘密情報を基に、新たな秘密情報を生成する秘密情報生成手段と、上記秘密情報生成手段で生成された新たな秘密情報に対応する新たなパラメータを生成するパラメータ生成手段と、上記署名、上記公開情報、上記共通の底、及び上記ディジタル情報から、新たな公開情報を生成する公開情報生成手段と、上記秘密情報生成手段で生成された新たな秘密情報、上記パラメータ生成手段で生成された新たなパラメータ、及び上記公開情報生成手段で生成された新たな公開情報を用いて、公開鍵暗号を実行する暗号実行手段とを備えることを特徴とする。

【００４７】第１４の発明は、上記第１１～１３の何れかの発明において、上記ディジタル署名方式は、請求項１～９の何れかに記載のディジタル署名方式であることを特徴とする。

【００４８】第１５の発明は、請求項１１～１４の何れかに記載の通信装置を含むシステムであることを特徴とする。

【００４９】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。

【００５０】まず、第１の実施の形態について説明する。

【００５１】本発明に係るディジタル署名方式は、例えば、図１に示すような通信システム１００により実施され、この通信システム１００は、本発明に係る情報通信システムを適用したものでもある。

【００５２】すなわち、通信システム１００では、証明書発行者Ｑ用端末装置２０と、ユーザｊ，ｉ，ｋを含む複数のユーザ用端末装置３０、４０、５０、・・・とがネットワーク１０上で接続されており、各端末装置は、ネットワーク１０を介して互いに通信するようになされている。また、通信システム１００には、各ユーザに共通の公開パラメータＰＶ（Public Values ）が管理されている公開データベースＰＤ（Public Database ）が設けられている。

【００５３】証明書発行者Ｑ用端末装置２０は、証明書発行者Ｑ固有の秘密鍵ｓQ （秘密情報）及び公開鍵ｖQ （公開情報）を生成する公開鍵生成部２１と、秘密鍵ｓQ 及び公開パラメータＰＶを用いて平文ｍに対する署名（匿名公開鍵証明書）を生成する署名生成部２２とを備えている。

【００５４】一方、ユーザ用端末装置３０、４０、５０、・・・は、各々同様の構成としている。例えば、ユーザｊ用端末装置３０は、ユーザｊ固有の秘密鍵ｓｊ及び公開鍵ｖｊを生成する公開鍵生成部３１と、平文ｍと上記署名の対応関係が正しいか否かを判別する判別部３２と、新たな署名を生成する署名生成部３３とを備えている。また、ユーザｊ用端末装置３０は、新たな署名を確認する確認部３５と、確認部３５で確認された新たな署名を用いて平文を暗号化する暗号化部３６と、確認部３５で確認された新たな署名を用いて暗号文を復号する復号部３４とを備えている。

【００５５】以下、上述のような通信システム１００の動作を上記図１及び図２を用いて説明する。尚、上記図２中の記号は、上記図５と同様の表記規則に従うものとする。

【００５６】ステップＳ２００：先ず、通信システム１００の共通のデータとして、大きな素数ｐ、Z_p^* の要素であり且つ位数ｐ－１のα、一方向性ハッシュ関数Ｈ０：Ｚ→Z_p ＼｛０｝を用いる。尚、ｐは、例えば、「$p > 2^{512}$ 」とする。これらのパラメータ（公開パラメータＰＶ（Public Values ））は、通信システム１００に参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースＰＤ（Public Database ）に登録されているものとする。そこで、証明書発行者（authority ）Ｑ用端末装置２０は、公開鍵生成部２１により、秘密鍵（復号鍵）ｓQ （$\in Z_{p-1}^*$ ）と、公開鍵（暗号化鍵）ｖQ （$=\alpha^{sQ} \bmod p$）とを生成し、公開鍵ｖQ を公開データベースＰＤに登録する。また、任意のユーザ用端末装置（ここではユーザ（User）ｊ用端末装置３０とする）は、公開鍵生成部３１により、秘密鍵（復号鍵）ｓｊ（$\in Z_{p-1}^*$ ）と、公開鍵（暗号化鍵）ｖｊ（$=\alpha^{sj} \bmod p$）とを生成し、公開鍵ｖｊを公開データベースＰＤに登録する。

【００５７】ステップＳ２０１：匿名公開鍵証明書の生成

証明書発行者Ｑ用端末装置２０は、署名生成部２２により、ユーザｊの公開鍵ｖｊを、乱数（random number ）ｋを用いて変換したｒを求め、平文ｍに対する署名（例えば、ＥｌＧａｍａｌ暗号によるディジタル署名）を生成する。具体的には、署名生成部２２は、乱数（秘密の乱数）ｋ（$k \in Z_{p-1}^*$ ）を選択し、

$r = v_j^k \bmod p$

$s = (H_0(m) - s_Q \cdot r) \cdot k^{-1} \bmod (p-1)$

なる計算を行う。この平文mに対するＥＩＧａｍａＩ暗号によるディジタル署名ｒ，ｓが匿名公開鍵証明書である。また、平文mは、その匿名公開鍵証明書の種類を示すパラメータとして使用できる。尚、匿名公開鍵証明書の種類を示すパラメータとしては、平文m或いは$H_0(m)$の代わりに、予め決められた固定値を使用してもよい。

【００５８】ステップＳ２０２：匿名公開鍵証明書の配送

次に、証明書発行者Ｑ用端末装置２０は、署名生成部２２で生成したディジタル署名ｒ，ｓと、その種類を示すパラメータmとを匿名公開鍵証明書（m，ｒ，ｓ）として、ユーザｊ用端末装置３０に対して送信する。

【００５９】ステップＳ２０３：これを受けたユーザｊ用端末装置３０は、判別部３２により、

$s_j' = s \cdot s_j^{-1} \bmod (p-1)$

を求め、

$\alpha^{H0(m)} \equiv v_Q^r \cdot r^{sj'} \pmod p$

が成り立つことを確認する。

【００６０】ステップＳ２０４：公開鍵暗号の利用

そして、ユーザｊ用端末装置３０は、

$\alpha^{H0(m)} \cdot v_Q^{-r} \equiv r^{sj'} \pmod p$

により、「ｒ」を底、「$\alpha^{H0(m)} \cdot v_Q^{-r} \bmod p$」を公開鍵、「$s_j'$」を秘密鍵として、離散対数問題に基づく公開鍵暗号を利用する。

【００６１】そこで、例えば、ＥＩＧａｍａＩ暗号によるディジタル署名を利用する場合について説明する。

【００６２】ステップＳ２０４（１）：ディジタル署名の生成

ユーザｊ用端末装置３０は、署名生成部３３により、平文m'に対する署名を以下のようにして生成する。

①署名生成部３３は、乱数k'（$\in Z_{p-1}^*$）を生成する。

②署名生成部３３は、

$r' = \alpha^{k'} \bmod p$

を計算する。

③署名生成部３３は、

$s' = (H_0(m') - s_j' \cdot r) \cdot (k')^{-1} \bmod (p-1)$

を計算する。

④そして、ユーザｊ用端末装置３０は、m'と、署名生成部３３で得られたｒ'及びｓ'を、証明書発行者Ｑ用端末装置２０からの匿名公開鍵証明書（m，ｒ）と共に通信相手（ここではユーザｉ用端末装置４０とする）に対して送信する。

【００６３】ステップＳ２０４（２）：署名検証

これを受けたユーザｉ用端末装置４０は、確認部４５により、

$r^{H0(m')} \equiv (\alpha^{H0(m)} \cdot v_Q^{-r})^{r' \cdot (r')^{s'}} \pmod p$

なる式が成立するかを確認する。そして、ユーザｉ用端末装置４０は、この確認ができた場合に、m'に対する署名は証明書発行者Ｑによって選ばれたユーザによって生成された署名であることを認識する。

【００６４】また、上述のステップＳ２０４：公開鍵暗号の利用としては、暗号化にも利用することができる。そこで、例えば、ユーザｋ用端末装置５０において、ＥＩＧａｍａＩ暗号による暗号化を行う場合について説明する。

【００６５】暗号化：ユーザｋ用端末装置５０は、暗号化部５６により、平文m"を以下のようにして暗号化する。

①暗号化部５６は、乱数k"を生成する。

②暗号化部５６は、

$C_1 = r^{k''} \bmod p$

を計算する。

③暗号化部５６は、

$C_2 = m'' \cdot (\alpha^{H0(m)} \cdot v_Q^{-r} \bmod p)^{k''} \bmod p$

を計算する。

④そして、ユーザｋ用端末装置５０は、暗号化部５６で得られたC_1及びC_2を、ユーザｊ用端末装置３０に対して送信する。

【００６６】復号：これを受けたユーザｊ用端末装置３０は、復号部３４により、

$m'' = C_2 / C_1^{sj'} \bmod p$

なる計算を行って、平文m"を得る。

【００６７】尚、上述のステップＳ２０４：公開鍵暗号の利用として、ＥＩＧａｍａＩ暗号を用いたものを説明したが、これに限らず、離散対数問題に基づく公開鍵暗号等を用いたものにも利用することができる。

【００６８】つぎに、第２の実施の形態について説明する。

【００６９】この第２の実施の形態では、上述した第１の実施の形態における通信システム１００に、ＥＩＧａｍａＩ暗号のディジタル署名方式の変形版を適用する。このため、第１の実施の形態では、ＥＩＧａｍａＩ暗号でｐ－１を用いて法演算を行うのに対して、第２の実施の形態では、素数ｑ（ｑはｐ－１を割り切る）を用いて法演算を行うという点が異なる。

【００７０】尚、この第２の実施の形態を実施する通信システム１００の構成については、上述した第１の実施の形態と同様であるため、その詳細な説明は省略する。以下、第１の実施の形態と異なる点についてのみ、図３を用いて具体的に説明する。

【００７１】ステップＳ３００：先ず、通信システム１００の共通のデータとして、大きな素数ｐ、ｑ（ｑはｐ－１を割り切る）、Z_p^*の要素であり且つ位数ｑのα、一方向性ハッシュ関数$H_0 : Z \rightarrow Z_q \setminus \{0\}$、H

$1 : Z_q \times Z \rightarrow \{0, \cdots, 2^t - 1\}$ を用いる。尚、ここでは、例えば、「$p > 2^{512}$」、「$q > 2^{160}$」、「$t > 72$」とする。これらのパラメータ（公開パラメータＰＶ）は、通信システム１００に参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースＰＤに登録されているものとする。

そこで、証明書発行者Ｑ用端末装置２０は、公開鍵生成部２１により、秘密鍵 s_Q（$\in Z_q \setminus \{0\}$）と、公開鍵 v_Q（$= \alpha^{s_Q} \bmod p$）とを生成し、公開鍵 v_Q を公開データベースＰＤに登録する。また、任意のユーザ用端末装置（ここではユーザ（User）ｊ用端末装置３０とする）は、公開鍵生成部３１により、秘密鍵 s_j（$\in Z_q \setminus \{0\}$）と、公開鍵 v_j（$= \alpha^{s_j} \bmod p$）とを生成し、公開鍵 v_j を公開データベースＰＤに登録する。

【００７２】ステップＳ３０１：匿名公開鍵証明書の生成

証明書発行者Ｑ用端末装置２０は、署名生成部２２により、ユーザｊの公開鍵 v_j を、乱数（random number）ｋを用いて変換したｒを求め、平文ｍに対する署名（例えば、ＥＩＧａｍａＩ暗号によるディジタル署名）を生成する。具体的には、署名生成部２２は、乱数（秘密の乱数）ｋ（$k \in Z_q \setminus \{0\}$）を選択し、

$$r = v_j^k \bmod p$$

$$s = (H_0(m) - s_Q \cdot r) \cdot k^{-1} \bmod q$$

なる計算を行う。この平文ｍに対するＥＩＧａｍａＩ暗号によるディジタル署名ｒ，ｓが匿名公開鍵証明書である。また、平文ｍは、その匿名公開鍵証明書の種類を示すパラメータとして使用できる。尚、匿名公開鍵証明書の種類を示すパラメータとしては、平文ｍ或いは $H_0(m)$ の代わりに、予め決められた固定値を使用してもよい。

【００７３】ステップＳ３０２：匿名公開鍵証明書の配送

次に、証明書発行者Ｑ用端末装置２０は、署名生成部２２で生成したディジタル署名ｒ，ｓと、その種類を示すパラメータｍとを匿名公開鍵証明書（ｍ，ｒ，ｓ）として、ユーザｊ用端末装置３０に対して送信する。

【００７４】ステップＳ３０３：これを受けたユーザｊ用端末装置３０は、判別部３２により、

$$s_j' = s \cdot s_j^{-1} \bmod q$$

を求め、

$$\alpha^{H0(m)} \equiv v_Q{}^r \cdot r^{s_j'} \pmod p$$

が成り立つことを確認する。

【００７５】ステップＳ３０４：公開鍵暗号の利用

そして、ユーザｊ用端末装置３０は、

$$\alpha^{H0(m)} \cdot v_Q{}^{-r} \equiv r^{s_j'} \pmod p$$

により、「ｒ」を底、「$\alpha^{H0(m)} \cdot v_Q{}^{-r} \bmod p$」を公開鍵、「$s_j'$」を秘密鍵として、離散対数問題に基づく公開鍵暗号を利用する。

【００７６】そこで、例えば、Ｓｃｈｎｏｒｒ暗号によるディジタル署名を利用する場合について説明する。

【００７７】ステップＳ３０４（１）：ディジタル署名の生成

ユーザｊ用端末装置３０は、署名生成部３３により、平文ｍ′に対する署名を以下のようにして生成する。

①署名生成部３３は、乱数ｋ′（$\in Z_q \setminus \{0\}$）を生成する。

②署名生成部３３は、

$$x = r^{k'} \bmod p$$

を計算する。

③署名生成部３３は、

$$e = H_1(x, m')$$

を計算する。

④署名生成部３３は、

$$y = k' - e \cdot s_j' \bmod q$$

を計算する。

⑤そして、ユーザｊ用端末装置３０は、ｍ′と、署名生成部３３で得られたｅ及びｙを、証明書発行者Ｑ用端末装置２０からの匿名公開鍵証明書（ｍ，ｒ）と共に通信相手（ここではユーザｉ用端末装置４０とする）に対して送信する。

【００７８】ステップＳ３０４（２）：署名検証

これを受けたユーザｉ用端末装置４０は、確認部４５により、

$$e = H_1(r^y \cdot (\alpha^{H0(m')} \cdot v_Q{}^{-r})^e \bmod p, m')$$

なる式が成立するかを確認する。そして、ユーザｉ用端末装置４０は、この確認ができた場合に、ｍ′に対する署名は、証明書発行者Ｑによって選ばれたユーザによって生成された署名であることを認識する。

【００７９】また、上述のステップＳ３０４：公開鍵暗号の利用としては、暗号化にも利用することができる。そこで、例えば、ユーザｋ用端末装置５０において、ＥＩＧａｍａＩ暗号による暗号化を行う場合について説明する。

【００８０】暗号化：ユーザｋ用端末装置５０は、暗号化部５６により、平文ｍ″を以下のようにして暗号化する。

①暗号化部５６は、乱数ｋ″を生成する。

②暗号化部５６は、

$$C_1 = r^{k''} \bmod p$$

を計算する。

③暗号化部５６は、

$$C_2 = m'' \cdot (\alpha^{H0(m)} \cdot v_Q{}^{-r} \bmod p)^{k''} \bmod p$$

を計算する。

④そして、ユーザｋ用端末装置５０は、暗号化部５６で得られた C_1 及び C_2 を、ユーザｊ用端末装置３０に対して送信する。

【００８１】復号：これを受けたユーザｊ用端末装置３

０は、復号部３４により、
$m'' = C_2 / C_1^{sj'} \bmod p$
なる計算を行って、平文m″を得る。
【００８２】尚、上述のステップＳ３０４：公開鍵暗号の利用として、Ｓｃｈｎｏｒｒ暗号やＥＩＧａｍａｌ暗号を用いたものを説明したが、これに限らず、離散対数問題に基づく公開鍵暗号等を用いたものにも利用することができる。
【００８３】つぎに、第３の実施の形態について説明する。
【００８４】この第３の実施の形態では、上述した第１の実施の形態における通信システム１００に、ＥＩＧａｍａｌ暗号のディジタル署名方式の変形版を適用する。すなわち、第３の実施の形態では、第１の実施の形態と同様に、匿名公開鍵証明書において平文m（平文mを元に計算して得たH0（m））を用いる際に、H0（m）＝０とする。
【００８５】尚、この第３の実施の形態を実施する通信システム１００の構成については、上述した第１の実施の形態と同様であるため、その詳細な説明は省略する。以下、第１の実施の形態と異なる点についてのみ、図４を用いて具体的に説明する。
【００８６】ステップＳ４００：先ず、通信システム１００の共通のデータとして、素数ｐ、Z_p^*の要素であり且つ位数ｐ－１のα、一方向性ハッシュ関数$H0 : Z \rightarrow Z_p \setminus \{0\}$を用いる。尚、ｐは、例えば、「ｐ＞２５１２」とする。これらのパラメータ（公開パラメータＰＶ）は、通信システム１００に参加している全てのユーザがアクセスすることができ、且つ不当な改ざん等が起こらないように適切に管理されている公開データベースＰＤに登録されているものとする。そこで、証明書発行者Ｑ用端末装置２０は、公開鍵生成部２１により、秘密鍵sQ（$\in Z_{p-1}^*$）と、公開鍵vQ（$=\alpha^{sQ} \bmod p$）とを生成し、公開鍵vQを公開データベースＰＤに登録する。また、任意のユーザ用端末装置（ここではユーザ（User）ｊ用端末装置３０とする）は、公開鍵生成部３１により、秘密鍵ｓｊ（$\in Z_{p-1}^*$）と、公開鍵ｖｊ（$=\alpha^{sj} \bmod p$）とを生成し、公開鍵ｖｊを公開データベースＰＤに登録する。
【００８７】ステップＳ４０１：匿名公開鍵証明書の生成
証明書発行者Ｑ用端末装置２０は、署名生成部２２により、ユーザｊの公開鍵ｖｊを、乱数（random number）ｋを用いて変換したｒを求め、ＥＩｇａｍａｌ暗号のディジタル署名の変形版、例えば、平文mをハッシュ関数の入力とした結果が「０」となるＥＩＧａｍａｌ暗号の署名を生成する。具体的には、署名生成部２２は、乱数（秘密の乱数）ｋ（$k \in Z_{p-1}^*$）を選択し、
$r = v_j^k \bmod p$
$s = sQ \cdot r \cdot k^{-1} \bmod (p-1)$
なる計算を行う。このディジタル署名ｒ，ｓが匿名公開鍵証明書である。
【００８８】ステップＳ４０２：匿名公開鍵証明書の配送次に、証明書発行者Ｑ用端末装置２０は、署名生成部２２で生成したディジタル署名ｒ，ｓを匿名公開鍵証明書（ｒ，ｓ）として、ユーザｊ用端末装置３０に対して送信する。
【００８９】ステップＳ４０３：これを受けたユーザｊ用端末装置３０は、判別部３２により、
$sj' = s \cdot sj^{-1} \bmod (p-1)$
を求め、
$vQ^r \equiv r^{sj'} \pmod p$
が成り立つことを確認する。
【００９０】ステップＳ４０４：公開鍵暗号の利用
そして、ユーザｊ用端末装置３０は、
$vQ^r \equiv r^{sj'} \pmod p$
により、「ｒ」を底、「$vQ^r \bmod p$」を公開鍵、「ｓｊ'」を秘密鍵として、離散対数問題に基づく公開鍵暗号を利用する。
【００９１】そこで、例えば、ＥＩＧａｍａｌ暗号によるディジタル署名を利用する場合について説明する。
【００９２】ステップＳ４０４（１）：ディジタル署名の生成
ユーザｊ用端末装置３０は、署名生成部３３により、平文m'に対する署名を以下のようにして生成する。
①署名生成部３３は、乱数ｋ'（$\in Z_{p-1}^*$）を生成する。
②署名生成部３３は、
$r' = \alpha^{k'} \bmod p$
を計算する。
③署名生成部３３は、
$s' = (H(m') - sj' \cdot r) \cdot (k')^{-1} \bmod (p-1)$
を計算する。
④そして、ユーザｊ用端末装置３０は、m'と、署名生成部３３で得られたｒ'及びｓ'を、証明書発行者Ｑ用端末装置２０からの匿名公開鍵証明書（m，ｒ）と共に通信相手（ここではユーザｉ用端末装置４０とする）に対して送信する。
【００９３】ステップＳ４０４（２）：署名検証
これを受けたユーザｉ用端末装置４０は、確認部４５により、
$r^{H0(m')} \equiv (vQ^r)^{r'} \cdot (r')^{s'} \pmod p$
なる式が成立するかを確認する。そして、ユーザｉ用端末装置４０は、この確認ができた場合に、m'に対する署名は、証明書発行者Ｑによって選ばれたユーザによって生成された署名であることを認識する。
【００９４】また、上述のステップＳ４０４：公開鍵暗号の利用としては、暗号化にも利用することができる。そこで、例えば、ユーザｋ用端末装置５０において、Ｅ

ＩＧａｍａＩ暗号による暗号化を行う場合について説明する。

【００９５】暗号化：ユーザｋ用端末装置５０は、暗号化部５６により、平文m″を以下のようにして暗号化する。

①暗号化部５６は、乱数ｋ″を生成する。

②暗号化部５６は、

$C_1 = r^{k''} \bmod p$

を計算する。

③暗号化部５６は、

$C_2 = m'' \cdot (v_Q{}^r \bmod p)^{k''} \bmod p$

を計算する。

④そして、ユーザｋ用端末装置５０は、暗号化部５６で得られたC_1及びC_2を、ユーザｊ用端末装置３０に対して送信する。

【００９６】復号：これを受けたユーザｊ用端末装置３０は、復号部３４により、

$m'' = C_2 / C_1^{sj'} \bmod p$

なる計算を行って、平文m″を得る。

【００９７】尚、上述のステップＳ４０４：公開鍵暗号の利用として、ＥＩＧａｍａＩ暗号を用いたものを説明したが、これに限らず、離散対数問題に基づく公開鍵暗号等を用いたものにも利用することができる。

【００９８】上述のように、本発明においては、ｐは素数、αの位数はｐ－１、$r \equiv v_j{}^k \equiv \alpha^{sjk} \pmod p$であり、$sj \in Z_{p-1}{}^*$、$k \in Z_{p-1}{}^*$である。或いは、ｐとｑが素数で、ｑはｐ－１を割り切り、αの位数がｑ、$r \equiv v_j{}^k \equiv \alpha^{sjk} \pmod p$であり、$sj \in Z_q \setminus \{0\}$、$k \in Z_q \setminus \{0\}$である。したがって、任意のｒが与えられたとき、そのｒは、どのユーザの公開鍵からも計算して得ることができる値であり、実際に使用されたｋの値が分からない限りは、どのユーザの公開鍵から計算して得られたのかは全く特定することができない。換言すれば、匿名公開鍵証明書である署名ｒには、どのユーザの匿名公開鍵証明書であるかを特定するための情報が一切含まれない。これにより、計算量的な上述した仮定２によってではなく、情報量的に匿名性が実現されており、仮定２が成り立たなくなる事態が起きたとしても、匿名性を確実に保つことができる。このため、プライバシー保護に関する安全性を向上させることができる。

【００９９】また、上述した何れの実施の形態においても、以下のように運用することで、プライバシー保護に関する安全性をさらに向上させることができる。

①証明書発行者Ｑ用端末装置２０は、任意のユーザ用端末装置（例えば、ユーザｊ用端末装置３０）に対して毎回異なる乱数ｋを用いた匿名公開鍵証明書を生成してユーザｊ用端末装置３０に対して送信する。

②これを受けたユーザｊ用端末装置３０は、ディジタル署名を生成せずに、１つの匿名公開証明書を異なる平文に対して使用する。このような、匿名公開鍵証明書を使用する方式（One-time Certificates 、使い捨て証明書方式）により、任意のディジタル署名を生成したユーザと、それとは別のディジタル署名を生成したユーザとが、同一のユーザであるか否かを判別することは、証明書発行者Ｑと、上記任意のディジタル署名を生成したユーザ以外のユーザとにとって、情報量的に非常に困難、すなわち不可能である。したがって、ユーザの匿名性は情報量的に保たれるため、プライバシー保護に関する安全性をさらに向上させることができる。

【０１００】

【発明の効果】以上説明したように本発明によれば、匿名公開鍵証明書である署名には、どのユーザの匿名公開鍵証明書であるかを特定するための情報が一切含まれない。これにより、計算量的な上述した仮定２によってではなく、情報量的に匿名性が実現されており、仮定２が成り立たなくなる事態が起きたとしても、匿名性を確実に保つことができる。したがって、プライバシー保護に関する安全性を向上させることができる。

【図面の簡単な説明】

【図１】第１の実施の形態において、本発明に係る情報通信システムを適用した通信システムの構成を示すブロック図である。

【図２】上記通信システムにおけるディジタル署名方式を説明するための図である。

【図３】第２の実施の形態において、上記通信システムにおけるディジタル署名方式を説明するための図である。

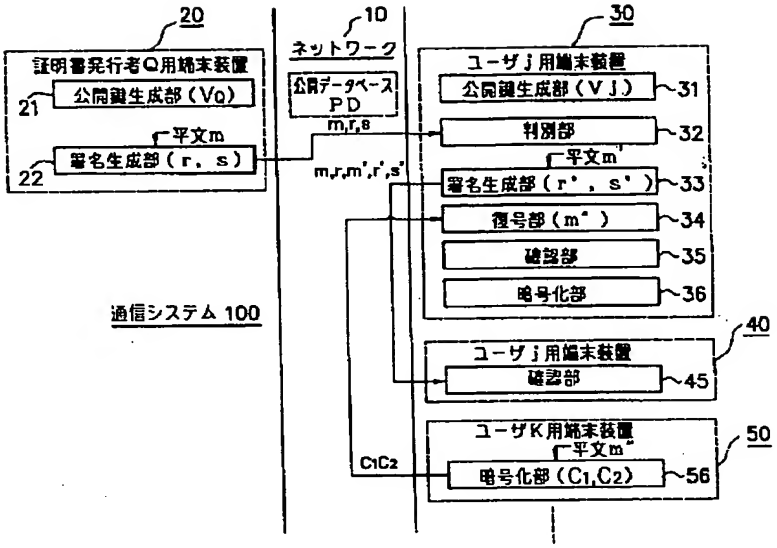
【図４】第３の実施の形態において、上記通信システムにおけるディジタル署名方式を説明するための図である。

【図５】従来のディジタル署名方式を説明するための図である。

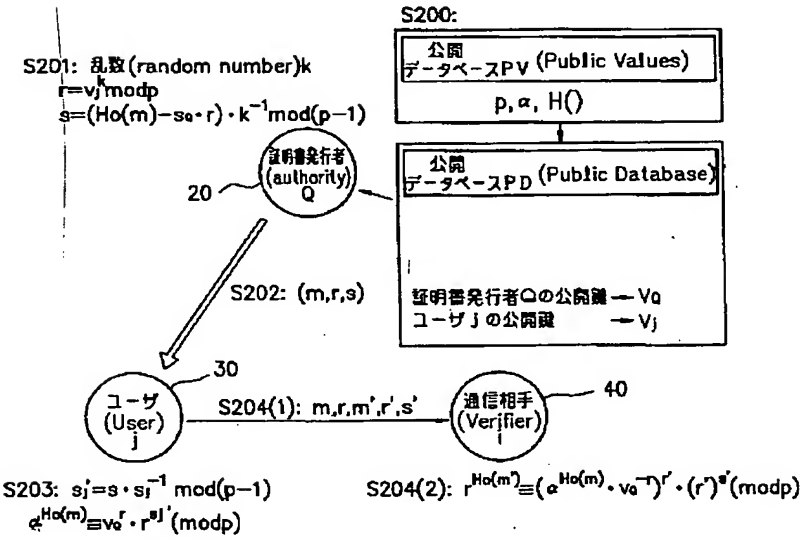
【符号の説明】

１０　ネットワーク
２０　証明書発行者用端末装置
２１　公開鍵生成部
２２　署名生成部
３０～５０　ユーザ用端末装置
３１　公開鍵生成部
３２　判別部
３３　署名生成部
３４　復号部
３５、４５　確認部
３６、５６　暗号化部

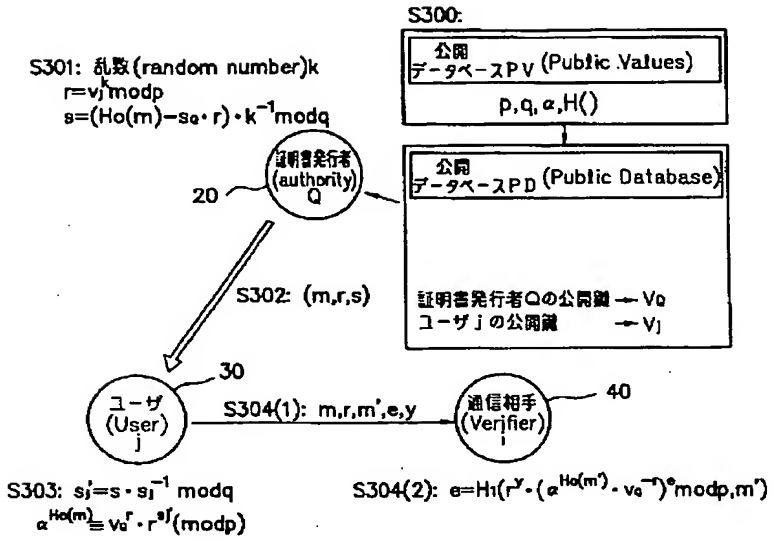
【図１】


20
10
30
証明書発行者Q用端末装置
ネットワーク
ユーザｊ用端末装置
公開鍵生成部（Vq）
21
公開データベース PD
公開鍵生成部（Vj）
31
m,r,s
判別部
32
平文m
署名生成部（r，s）
22
m,r,m',r',s'
平文m'
署名生成部（r'，s'）
33
復号部（m''）
34
確認部
35
暗号化部
36
通信システム 100
40
ユーザｊ用端末装置
確認部
45
ユーザK用端末装置
50
C1C2
平文m''
暗号化部（C1,C2）
56

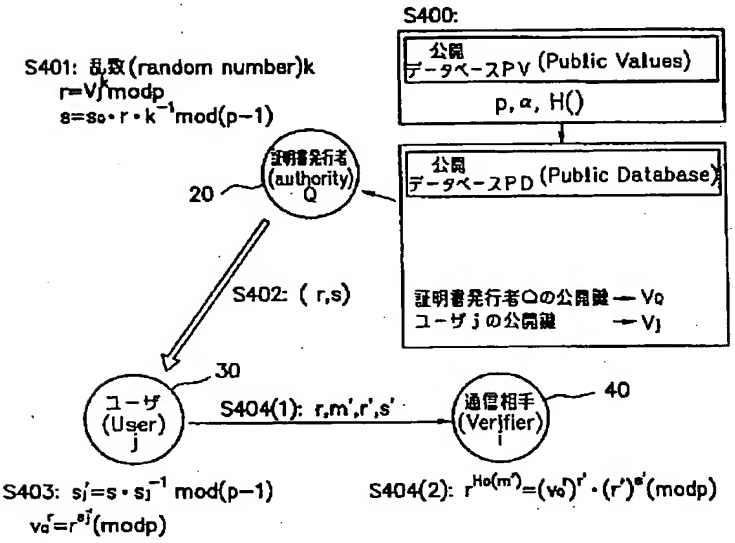
【図２】


S200:
公開 データベースPV (Public Values)
p, α, H()
S201: 乱数(random number)k
r=vj^k mod p
s=(Ho(m)−sq・r)・k^−1 mod(p−1)
証明書発行者 (authority) Q
20
公開 データベースPD (Public Database)
S202: (m,r,s)
証明書発行者Qの公開鍵 — Vq
ユーザｊの公開鍵 — Vj
30
ユーザ (User) j
S204(1): m,r,m',r',s'
通信相手 (Verifier) i
40
S203: sj'=s・sj^−1 mod(p−1)
α^Ho(m) ≡ Vq^r・r^sj' (modp)
S204(2): r^Ho(m') ≡ (α^Ho(m)・Vq^−r)^r'・(r')^s' (modp)

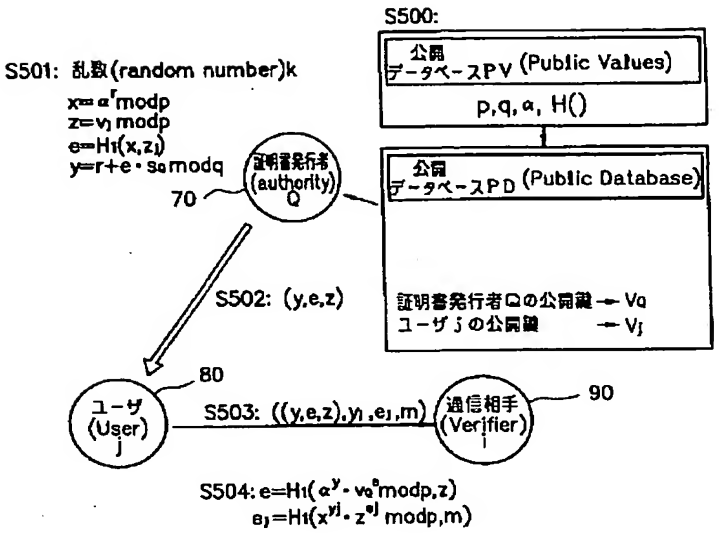
【図３】


S300:
公開データベースPV (Public Values)
p,q,α,H()
公開データベースPD (Public Database)
証明書発行者Qの公開鍵 → Vq
ユーザjの公開鍵 → Vj
S301: 乱数(random number)k
r=vj^k modp
s=(Ho(m)−sq・r)・k^−1 modq
証明書発行者 (authority) Q
20
S302: (m,r,s)
30
ユーザ (User) j
S304(1): m,r,m',e,y
通信相手 (Verifier) i
40
S303: sj'=s・sj^−1 modq
α^Ho(m) ≡ vq^r・r^sj (modp)
S304(2): e=H1(r^y・(α^Ho(m')・vq^−r')^e modp,m')

【図４】


S400:
公開データベースPV (Public Values)
p,α, H()
公開データベースPD (Public Database)
証明書発行者Qの公開鍵 → Vq
ユーザjの公開鍵 → Vj
S401: 乱数(random number)k
r=Vj^k modp
s=sq・r・k^−1 mod(p−1)
証明書発行者 (authority) Q
20
S402: (r,s)
30
ユーザ (User) j
S404(1): r,m',r',s'
通信相手 (Verifier) i
40
S403: sj'=s・sj^−1 mod(p−1)
vq^r=r^sj (modp)
S404(2): r^Ho(m')=(vq^r')^r'・(r')^s' (modp)

【図５】


S500:
公開
データベースPV (Public Values)
p,q,α, H()
公開
データベースPD (Public Database)
証明書発行者Qの公開鍵 → Vq
ユーザjの公開鍵 → Vj
S501: 乱数(random number)k
x=α^r modp
z=vj modp
e=H1(x,zj)
y=r+e・sa modq
証明書発行者
(authority)
Q
70
S502: (y,e,z)
80
ユーザ
(User)
j
S503: ((y,e,z),yj ,ej,m)
通信相手
(Verifier)
i
90
S504: e=H1(α^y・vq^e modp,z)
ej=H1(x^yj・z^ej modp,m)